类 BAN 逻辑基本模型及缺陷*

许剑卓，戴英侠，左英男

(中国科学技术大学研究生院 信息安全国家重点实验室，北京 100039)

E-mail: jzxu@163.net; dyx1234@sina.com

http://www.home.is.ac.cn

摘要：类 BAN 逻辑是一种用于分析密码协议安全性的逻辑.在分析了 BAN,AT,MB,GNY,SVO 等类 BAN 逻辑之后，指出这些逻辑的缺陷，包括若干新发现的缺陷.首先把类 BAN 的模型抽象出来，形成一个五元组模型，然后分析该模型的各个要素，并依据该模型对类 BAN 逻辑的缺陷进行分类，最后指出进一步发展类 BAN 逻辑应解决的问题.

关键词：密码协议;BAN 逻辑;缺陷

中图法分类号：TP393 **文献标识码**：A

密码协议利用密码学手段来实现密钥交换和身份认证，是一切安全通信的基础.随着密码协议的不断发展，协议也日趋复杂，人工对协议的分析往往无法保证协议的安全性.同时，密码协议本身具有的特性使其适合用形式化方法进行分析.因此，使用形式化方法对密码协议进行分析这一学科便应运而生.20 世纪 80 年代末，在 Burrow,Abadi,Needham 提出 BAN 逻辑[1]之后，基于逻辑和信念的形式化分析方法就成为研究的焦点.

类 BAN 逻辑分析密码协议的方法是针对协议的消息，分析协议的用户在接收到协议消息后能形成的信念，从而判断在协议结束时能否达到协议的既定目的.BAN 逻辑并不是一个完善的逻辑，它存在着很多错误和不足，比如在 BAN 逻辑提出不久，Nesset 即指出 BAN 逻辑存在严重的缺陷[2].因此，很多研究者在 BAN 逻辑的基础上发展了新的逻辑，如 AT 逻辑[3],MB 逻辑[4],GNY 逻辑[5],SVO 逻辑[6]等.这些逻辑一方面在推理逻辑上消除 BAN 逻辑存在的不正确或不严格的推理法则，另一方面采用更为严格的形式化技术证明逻辑自身的正确性.但是，一方面，由于 BAN 逻辑本身模型的原因限制了 BAN 逻辑的应用范围，这使得有些缺陷在现有的 BAN 逻辑模型下是无法消除或难以消除的；另一方面，在类 BAN 逻辑中往往注重从逻辑上消除推理法则的错误，而并没有提出实际可操作的方法.因此，有必要分析类 BAN 逻辑当前存在的缺陷问题，并指出以后发展的基本思路.

本文第 1 节为类 BAN 逻辑提炼出一个共同的模型并对 BAN 逻辑给出一个简单介绍.第 2 节分析类 BAN 逻辑中存在的缺陷，并依照逻辑的基本模型把这些缺陷分为 5 类，同时给出这些缺陷的具体例子.第 3 节指出进一步发展类 BAN 逻辑潜在的方法.

1 类 BAN 逻辑

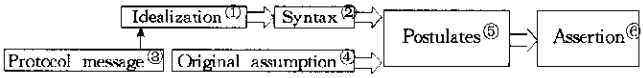
类 BAN 逻辑由一组推理法则组成.这组法则用来推导用户能够从接收到的消息中能获得的信念(belief)，下面将分别描述类 BAN 逻辑的基本模型、符号及其含义、部分推理法则.由于篇幅的限制，不可能对各个类 BAN 逻辑进行详细的描述，因此在后续的对类 BAN 逻辑的分析中只能给出引用到的部分，具体对类 BAN 逻辑的描述请参照文献[1,3~6].

* 收稿日期：1999-06-25；修改日期：1999-09-21

作者简介：许剑卓(1977－)，男，广东汕头人，硕士生，主要研究领域为计算机网络安全；戴英侠(1942－)，女，安徽肖县人，教授，主要研究领域为信息安全；左英男(1973－)，男，河北石家庄人，硕士生，主要研究领域为计算机网络安全.

1.1 类 BAN 逻辑的基本模型

对所有的类 BAN 逻辑进行分析,我们发现类 BAN 逻辑在基本模型上都是一致的,如图 1 所示.



①理想化处理,②符号,③协议消息,④初始假设,⑤推理法则,⑥断言.

Fig. 1 The model of BAN family of logic

图1 类BAN逻辑的基本模型

图 1 中各要素的定义如下:

(1) 协议消息(protocol message).依照协议规定某个协议的实体所能接收到的消息.这是协议分析最为原始的素材.

(2) 理想化方法(idealization).因具体的协议描述方法多种多样,同一消息在不同的协议中可能有不同的含义,因此,需要把具体的协议的各条消息转化为推理逻辑所能处理的没有歧义性的符号,这个转换过程就称为理想化处理过程,或简称理想化过程.在实际应用中,理想化方法不仅产生符号序列,有时还能直接获得部分断言.

(3) 符号(sytax).用于描述消息的集合,它是推理逻辑可直接处理的消息符号.往往每一种逻辑都定义了自己所能处理的符号集,通常又称该符号集为语言.各个逻辑定义的语言各不相同,通常都由一组最为简单的初始符号通过一定的生成规则生成.

(4) 初始假设(original assumption).通常每一种逻辑的使用都对协议的外部特性有一定的假设,这些假设构成了初始假设集合.比如,对算法安全性的假设、对共享秘密保密性的假设等.

(5) 推理法则(postulates).推理逻辑由一组推理法则构成,这些推理法则在初始假设的基础上推断,从输入符号中能推断出怎样的断言.它们是逻辑的核心部分.

(6) 断言(assertion).断言是推理逻辑的结果,所有断言构成了断言集合.这些断言描述了协议用户对自身以及与其通信用户的状态(信念)或动作的推断.

由上述分析可以看出,每一种逻辑由符号集合,断言集合,初始假设,推理逻辑,理想化方法这样一个五元组构成,对一种逻辑的分析应从这 5 个方面着手.具体协议的各个要素将在本文后续部分加以中描述.

1.2 BAN 逻辑的符号含义

惯例上常用大写字母如 A,B,P,Q 等表示通信实体;用 K_{ab} 表示通信实体 A 和 B 共享的通信密钥;用 K_a,K_b 表示 A 和 B 的公钥;用 K_a^{-1},K_b^{-1} 表示 A 和 B 的私钥;用 $\{X\}_K$ 表示用密钥 K 加密消息 X 的结果.

在 BAN 逻辑中引入以下符号:

$P\models X$:P 相信 X.P 认为 X 为真.

$P\lhd X$:P 看见 X.P 收到包含 X 的消息.

$P\mid\sim X$:P 曾经说过 X.这个断言包含两个含义:一方面是指消息 X 是由 P 发出的,即消息源是 P.另一方面是指 P 能够确认消息 X 的含义,也即能够识别该消息并对该消息做出正确的解释,对此,后文将进一步加以解释.

$\#(X)$:X 是新的(fresh),在这一轮协议执行之前未被传送过,如时戳、随机数等.

$P\overset{K}{\longleftrightarrow}Q$:$P$ 和 Q 可使用 K 进行秘密通信,而且 K 为好的(good)密钥.这个断言是指密钥的排他性,也即只有 P,Q 或可信任的第三方知道 K.

$Q\Rightarrow X$:表示 Q 对 X 有管辖权(jurisdiction).比如,由第三方生成通信密钥时,则称第三方对密钥的生成有管辖权.

1.3 BAN 逻辑的推理法则

在 BAN 逻辑中通过一系列的推理法则分析理想化得到的符号序列,从而推导协议用户的信念(belief).下面给出在 BAN 逻辑中最重要的推理法则.

1.3.1 消息意义法则

$$\frac{P \models P \xleftrightarrow{K} Q, P \lhd \{X\}_k}{P \models Q \sim X}$$

该推理法则的含义是,若 P 接收到用 k 加密的消息 $\{X\}_k$,且 k 为 P 和 Q 的共享密钥,那么可断言 X 为 Q 发出的消息,且 P 能够理解该消息的含义.

1.3.2 管辖权法则

$$\frac{P \models Q \Rightarrow X, P \models Q \mid\sim X}{P \models X}$$

这条推理反映了现实中的信任关系.也即如果 P 在 X 方面信任 Q,那么 Q 说什么,P 就相信什么.

1.3.3 Nonce 检验法则

$$\frac{P \models Q \mid\sim X, P \models \#(X)}{P \models Q \models X}$$

该推理法则的意思是,假如 Q 曾经说过 X,而且 X 是新的,那么可以推断 Q 相信 X.这是 BAN 逻辑中可以推导对方通信实体信念的推理法则.

1.3.4 时新性法则

$$\frac{P \models \#(X)}{P \models \#(X,Y)}$$

这条消息的含义是,若消息的一部分是新的,那么整个消息也是新的.

2 类 BAN 逻辑存在的缺陷

类 BAN 逻辑都是通过消除 BAN 逻辑中的一些缺陷而进一步向前发展的,类 BAN 逻辑的设计者都没有对类 BAN 逻辑的缺陷进行全面的分析,而是针对 BAN 逻辑的某个缺陷进行改进,这使得任何一个类 BAN 逻辑中都多多少少地存在一些 BAN 逻辑中存在的缺陷.因此,在进一步发展类 BAN 逻辑之前,有必要在类 BAN 逻辑模型的基础上分析其缺陷并进行归类.

逻辑中的推理法则实际上是对现实中分析协议的方法的抽象,而逻辑处理的符号集合则是对现实协议的抽象.同样,初始假设、断言集合都是从现实体系中抽象出来的要素.针对符号集合、断言集合、初始假设、推理逻辑、理想化方法这 5 个要素分别导致 BAN 逻辑的不同缺陷,分别叙述如下.

2.1 由于符号集合、断言集合定义引起缺陷

在 BAN 逻辑中并没有严格而明确地定义其分析的符号集合和作为分析结果的断言集合,甚至可以说没有区分这两个集合的含义.但在类 BAN 逻辑中大多用严格的形式化的方法定义这两个集合.符号集合是对现实协议的抽象,而断言集合则是对分析结果的抽象,因此,对这两个集合的定义可以说是逻辑的基础特性之一.这两个集合的定义必将导致以下缺陷.

缺陷类型 1:符号集合定义限制了逻辑所能处理的协议范围.

符号集合定义了协议的消息,是通过理想化过程从协议消息抽象而来的.对符号集合的定义就限定了逻辑所能处理的协议范围.比如下面的几个实例.

实例 1:BAN,AT,GNY,SVO,MB 逻辑无法分析由时间同步问题所引起的协议缺陷.

很多协议的缺陷是由于时间不同步引起的,比如在 Kerberos 协议中,若时间不同步则可能使攻击者冒充合法用户通过身份认证[7].而在类 BAN 逻辑中并没有引入描述时间的符号,这就使得任何与时间相关的协议缺陷都不在 BAN 逻辑分析范围内.Syverson 在文献[8]中提出一种把时间作为一个要素加入逻辑的方法,但该技术在目前仍很不成熟.

实例 2:BAN,AT,GNY,MB 逻辑无法分析使用 Diffie Hellman 等特殊密钥交换算法交换密钥的协议.

类 BAN 逻辑分析的主要对象是密钥交换协议,但这些逻辑只考虑了用非对称密码体制或基于共享秘密的密钥交换方式,而没有考虑 Diffie Hellman 等密钥交换方式,这限制了逻辑的处理范围.在 SVO 逻辑中引入新的符号表示密钥交换密钥以解决整个问题.

缺陷类型 2:断言集合的定义限定了逻辑的分析能力.

断言集合通常由主体、谓语、对象 3 个部分组成.在不同的逻辑中定义了不同的谓语.比如,在 BAN 逻辑中有 $|\equiv$(believe),$<$(see),$|\sim$(said);在 AT 逻辑中,则在 BAN 逻辑基础上引入了 says 和 has 这两个谓语;在 GNY 逻辑中有引入了 possess 谓语.定义的断言集合若不能反映现实的协议模型,则会使逻辑的分析能力受到限制.

实例 3:在 BAN 逻辑的成立要求以诚实性为前提.

BAN 逻辑的 Nonce 检验法则认为,若通信实体 Q 曾经说过 X 且 X 为新的,那么可断定 Q 相信(believe)X.而实际上这只能断定 Q 刚刚说过 X,因为在 BAN 逻辑中没有引入 says 的概念.因此,要使 BAN 逻辑的 Nonce 检验法则成立,则要求存在以下诚实性假设:若 P 刚说过 X,那么 P 相信 X,也即通信实体只发出它相信的消息.换句话说,任何通信实体都不说谎.

这一问题在后续的类 BAN 逻辑中基本上已得到解决.

2.2 不合理的推理法则和初始假设引起的缺陷

在类 BAN 逻辑中,推理法则实际上就是一套公理,也就是说,它们的正确性是以人们的经验为基础的,而不是能够证明的.正是由于它以人的经验为基础,所以难免存在与事实不符的地方.这种缺陷又分为两类,推理法则缺陷和初始假设缺陷.如果一个推理法则的错误可以通过引入一定的初始假设使它变为正确的推理法则,则称该缺陷为初始假设缺陷,也即若原推理法则 $A\Rightarrow B$ 是错误的,其引入假设 C,使得 $(A,C)\Rightarrow B$ 是正确的,则可称其为初始假设缺陷.若推理法则作为一个公理体系本身就存在逻辑错误(也即用这套公理能推出错误的结论),或者推理法则不以事实为根据,则称其为推理法则缺陷.

缺陷类型 3:初始假设缺陷

初始假设缺陷已为大多数研究者所注意,而且在类 BAN 逻辑中大多试图改正 BAN 逻辑存在的初始假设缺陷.在 BAN 逻辑中存在很多初始假设缺陷,有必要对这些缺陷进一步进行归类分析.此处只给出一个典型的例子.

实例 4:消息不可伪造假设.

在 BAN 逻辑中,消息意义法则的含义是:若 P 接收到用 k 加密的消息 $\{X\}_k$,且 k 为 P 和 Q 的共享密钥,那么可断言 X 是 Q 发出的消息,且 P 能够理解该消息的含义.实际上,该推理法则要求以下假设成立:

(消息不可伪造假设)任何不知道 k 的第三方无法伪造出格式为 $\{X\}_k$ 的消息.

这里,消息的格式是指对消息的解释方法;伪造包括各种各样的方法,如消息重播、蛮力攻击等方法.比如,对于协议中有消息 $\{A,B,Kab\}_k$ 和 $\{A,B,Nc\}_k$,若通信实体预期接收到消息 $\{A,B,Kab\}_k$,而攻击者用 $\{A,B,Nc\}_k$ 冒充该消息,那么消息接收者则把格式为 $\{A,B,Nc\}_k$ 的消息当成格式 $\{A,B,Kab\}_k$ 来解释,因此把 Nc 解释为 Kab,这就称为用格式为 $\{A,B,Nc\}_k$ 伪造格式为 $\{A,B,Kab\}_k$ 格式的消息.很显然,若不知道 k 的第三方能伪造出格式为 $\{X\}_k$ 的消息,那么,若接收到消息 $\{X\}_k$,则不能断定该消息一定是 Q 发出的,还有可能是第三方伪造的.上述假设意味着 BAN 逻辑无法分析伪造消息可能引起的协议缺陷.

类 BAN 逻辑一直在试图消除这一缺陷,也即使得逻辑本身能够判断不知道 k 的第三方是否能够伪造格式为 $\{X\}_k$ 的消息.但是,由于伪造消息的方法多种多样而使得消除这一缺陷相当困难.而且在大多数类 BAN 逻辑中只是把消息伪造理解为消息重播,这使得类 BAN 逻辑对 BAN 逻辑的改正不具有彻底性.

缺陷类型 4:推理法则缺陷.

在有些类 BAN 逻辑中作为公理体系的推理法则本身不符合逻辑或与事实不符,这种缺陷称为推理法则缺陷.在发展类 BAN 逻辑时,逻辑的设计者按照自己的经验去构造逻辑,而这使得逻辑中难免存在一些与现实不符的情况.这往往出现在类 BAN 逻辑中,而这些问题还没有引起研究者的广泛注意.例如,在 GNY 逻辑中,我们发现存在以下缺陷:

实例 5:GNY 逻辑中的可识别性判断法则存在推理法则缺陷.

前面已指出,消息意义法则要求以消息不可伪造假设为前提,而在 GNY 逻辑中把它总结为消息可识别性假设.在 GNY 逻辑中所谓消息可识别是指,消息的接收者能够判定消息的格式.具体地说,消息 $\{X\}_k$ 具有可识

别性即是指,(1) 用户能够判断出该消息确实是以 k 加密的信息,比如通过加入冗余信息保证;(2) 保证该消息确实是本协议本轮次本序号的消息.在 GNY 逻辑中为判定消息是否具有可识别性提出了若干推理法则.在此处不具体解释各个推理法则的含义,只举例说明其存在的错误.在 GNY 逻辑中存在以下 3 个推理法则:

$$R6:\frac{P\ni H(x)}{P\models\varphi(x)},\quad P4:\frac{P\ni X}{P\ni H(x)},\quad P1:\frac{P\lhd X}{P\ni X}$$

由这 3 个推理法则可以综合得到 $\frac{P\lhd X}{P\models\varphi(X)}$,其中 $P\lhd X$ 表示 P 接收到消息 X,而 $\varphi(X)$ 表示消息 X 是可识别的.按照以上结论,即 P 能够识别所接收到的任何消息.显然,这是很荒谬的结论.这一缺陷是由于推理法则 $R6$ 没有现实的逻辑基础造成的.这一类型的推理法则缺陷在其他类 BAN 逻辑中也同样存在,在此不再赘述.

2.3 理想化方法引起的缺陷

由于相同的消息在不同的协议中可能代表不同的意义,因此,在使用逻辑分析协议之前必须对协议进行理想化处理,也即用逻辑所能处理的语言描述协议,以形成无二义性的描述.但是,在 BAN,AT,GNY,SVO 逻辑中并没有给出具体怎样把一个协议转化为它能处理的方式,也即在这些逻辑中并没有定义严格的理想化方法.只有在 MB 逻辑中给出了一定的理想化步骤,但这仍然不是一个有效的方法.因此,在用逻辑分析协议的安全性之前还必须由逻辑的使用者凭个人经验对协议进行理想化操作,这使得对协议的分析结果是否正确在很大程度上依赖于分析者对协议的理想化方式是否正确.例如,在文献[4]中就指出了 BAN 逻辑的设计者在理想化 Otway-Rees 协议时存在着错误.

缺陷类型 5:在所有类 BAN 逻辑中均未给出有效的理想化方法.

理想化方法的欠缺使得逻辑这种形式化方法建立在非形式化的基础上.这使得逻辑只能为少数专家使用,而且也阻碍了用计算机自动分析协议安全性,完全违背了形式化方法的目的.因此,在使用计算机自动分析协议安全性之前有必要先对协议的理想化方法作进一步的研究.一种潜在的解决方法是,在设计协议时使用逻辑定义的语言描述协议并进行分析,然后再把该描述的结果转化为现实的通信协议.

缺陷类型 6:类 BAN 逻辑无法分析依赖于实现的缺陷.

协议缺陷可分为功能性缺陷(functional specification flaw)、依赖于实现的缺陷(implementation dependent flaw)和实现缺陷(implementation flaw).由于在类 BAN 逻辑的模型中,逻辑分析的对象不是最终投入使用的消息,而是经过抽象了的符号.这使得由该模型发展而来的任何逻辑只能分析出功能性缺陷.文献[9]中给出了一种可分析依赖实现缺陷的逻辑,但该技术是否可行仍有待于进一步研究.

3 类 BAN 逻辑亟待解决的问题

前面,我们对类 BAN 逻辑存在的缺陷进行了分类并给出若干具体的缺陷.由此可以看出,类 BAN 逻辑还很不完善,还存在很多亟待解决的问题.类 BAN 逻辑的不断发展促进了人们对很多问题的进一步探索,这些问题已超越了类 BAN 逻辑本身,是整个密码学所需解决的问题,这些问题的解决是进一步发展类 BAN 逻辑的前提.它们主要有:

- 必须明确认证协议的目的是什么,也即用户通过认证协议的运行最后应达到怎样的信念才算认证成功.对于认证的目的,应用逻辑定义的语言加以描述.文献[10]对这一问题做了有益的探索.
- 必须明确什么是协议缺陷.在分析协议时,有时连究竟什么是协议缺陷都很难解释清楚,因此,有必要用形式化的语言来描述究竟什么是协议缺陷.
- 建立可操作的理想化方法.
- 建立通用的描述协议的语言以排除协议的二义性.
- 完善逻辑的推理法则,并证明该推理法则的正确性.

在实现由计算机自动分析协议安全之前,这些问题都是无法回避的问题.此外,还有很多其他问题需要解决,限于篇幅,本文不再一一赘述,仅列出其中最为重要的部分.

References:

[1] Burrows, M., Abadi, M., Needham, R. A logic of authentication. Technical Report 39, Digital Systems Research Center, 1989.

[2] Nessett, D. M. A critique of the burrows, abadi, and needham logic. Operating Systems Review, 1990,4(2):35~38.

[3] Abadi, M., Tuttle, M. A semantics for a logic of authentication. In: Ley, M. ed. Proceedings of the 10th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1991. 201~216.

[4] Mao, Wen-bo, Boyd, C. Towards a formal analysis of security protocols. In: Jackson, R. ed. Proceedings of the Computer Security Foundations Workshop VI. Los Alamitos, CA: IEEE Computer Society Press, 1991. 147~158.

[5] Li, Gong, NeedHam, R., Yahalom, R. Reasoning about belief in cryptographic protocols. In: Mike, C. C., ed. Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1990. 234~248.

[6] Syverson, P. F., van Oorschot, P. C. On unifying some cryptographic protocol logics. In: Oakson, N. ed. Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press. 1994. 109~121.

[7] Bellovin, S. M., Merritt, M. Limitations of the kerberos authentication system. Computer Communication Review, 1990,20(5):119~132.

[8] Syverson, P. F. Adding time to a logic of authentication. In: Niko Bari'c ed. Proceedings of the 1st ACM Conference on Computer and Communications Security. New York: ACM Press, 1993. 97~101.

[9] Carlsen, U. Using logics to detect implementation-dependent flaws. In: Narret, P. ed. Proceedings of the 9th Annual Computer Security Applications Conference. Los Alamitos, CA, IEEE Computer Society Press, 1993. 64~73.

[10] Boyd, C. Towards extensional goals in authentication protocols. In: Meadows, C. ed. Proceedings of the DIMACS Workshop on Cryptographic Protocol Design and Verification. Piscataway, NJ: Rutgers Press, 1997. 291~303.

The Model and Its Defects of BAN Family of Logic

XU Jian-zhuo, DAI Ying-xia, ZUO Ying-nan

(*State Key Laboratory of Information Security, Graduate School of University of Science and Technology of China, Beijing* 100039, *China*)

E-mail: jzxu@163.net; dyx1234@sina.com

http://www.home.is.ac.cn

Received June 25, 1999; accepted September 21, 1999

Abstract: BAN family of logic is used to analyze the security of cryptographic protocols. Five logics in the BAN family of logic are analyzed, including GNY, AT91, MB, SVO and BAN logic itself. Many defects of BAN family of logic are presented, including some defects found in research. A model is presented to describe the BAN family of logic first. And then the defects of BAN family of logic are classified according to this model. Some problems concerning BAN family of logic are presented in order to stimulate further research.

Key words: cryptographic protocol; BAN logic; defect